ARMY RESEARCH LABORATORY

Network Basic Language Translation System: Security Infrastructure

by Mark R. Mittrick

ARL-MR-668 **July 2007**

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Aberdeen Proving Ground, MD 21005-5067

ARL-MR-668 **July 2007**

Network Basic Language Translation System: Security Infrastructure

Mark R. Mittrick
Computational & Information Sciences Directorate, ARL

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
July 2007	Final	September 2005–May 2006

4. TITLE AND SUBTITLE
Network Basic Language Translation System: Security Infrastructure

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mark R. Mittrick

5d. PROJECT NUMBER
611102H48

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: AMSRD-ARL-CI-CT
Aberdeen Proving Ground, MD 21005-5067

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-MR-668

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Department of Defense Horizontal-Fusion program was created in 2003 to usher in a new era in defense computation and communications. The Network Basic Language Translation System (NetBLTS) was proposed and accepted as part of the U.S. Army Research Laboratory's offering of initiatives within the Horizontal Fusion portfolio in 2003. This report provides an overview of NetBLTS components, including associated hardware and software, the architecture of the system, data storage, the secure facilities, security requirements, and availability of the system, with the focus on security issues and the difficulties created by them.

15. SUBJECT TERMS
NetBLTS, security, horizontal fusion, machine language translation, system administration

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mark R. Mittrick
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL	28	19b. TELEPHONE NUMBER (*Include area code*) (410) 278-4148

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

Acknowledgments

This report would not have been possible without the efforts of Tactical Collaboration and Data Fusion Branch members, as well as the NetBLTS team, which includes: Mr. Eric Heilman, Mr. Gary Moss, Mrs. Janet O'May, and Mr. John Richardson.

1. Introduction

The Department of Defense (DOD) program, Horizontal Fusion (HF), was created in 2003 to usher in a new era in defense computation and communications. The Networked Basic Language Translation System (NetBLTS) was proposed and accepted as part of the U.S. Army Research Laboratory's (ARL's) offering of initiatives within the HF portfolio in 2003.

> "NetBLTS enables non-linguists to quickly triage foreign documents and provides a translation aid to linguists. NetBLTS provides Optical Character Recognition (OCR), machine translation, and document management and indexing. Users can save extracted keywords and phrases, document translations, and foreign documents to a database repository for future analysis. The repository is accessible through the Horizontal Fusion Federated Search application."[1]

An updated system security plan (SSP) was required for all HF initiatives. The SSP for NetBLTS provided information on all associated hardware and software, the architecture of the system, data storage, the secure facilities, security requirements, and availability of the system.

In the next several sections, we will talk about these various components and the difficulties created by them.

2. Background

The NetBLTS team worked in the DOD zero-tolerance security environment. In the event of any security infraction, the NetBLTS application had to be taken immediately offline to correct the deficiency.

The NetBLTS team worked with other HF teams (such as the test and integration team at Space and Naval Warfare in South Carolina and the HF production and the HF management teams in Virginia), to develop and test new NetBLTS application features. Throughout the software development cycle, the NetBLTS code went through different stages of testing to ensure security and operability.

[1] Horizontal Fusion Portfolio Partners and Initiatives. http://horizontalfusion.dtic.mil/initiatives/page2.html (accessed 1 February 2007).

3. Hardware and Software

The NetBLTS computer servers consisted of five Dell PowerEdge* rack-mounted systems:

- NETBLTSDB4 (PowerEdge 2850) primary web and database (DB) server
- NETBLTS4WK1 (PowerEdge 2650) language-translation and backup server
- NETBLTS4WK2 (PowerEdge 2650) language-translation server
- NETBLTS4WK3 (PowerEdge 2650) language-translation server
- NETBLTS4WK4 (PowerEdge 2650) language-translation server

Each server ran the Windows Server 2003† operating system plus HighView‡ workflow software, developed by CACI. NETBLTSDB4 hosted the Oracle§ database and the Microsoft Internet Information Server.** NETBLTSWK1–NETBLTSWK4 shared the language translation load. This gave the NetBLTS system redundancy in case of a failure and allowed it to distribute the backend processing load. The Oracle database software was selected because of its structural-query language extensions, which support Google-like†† searches of stored documents. The Oracle database stored previously translated documents, as well as the Universal Description, Discovery and Integration (UDDI) binding cache service profiles.

4. Facility Security

The NetBLTS team was based at the U.S. Army Aberdeen Proving Ground (APG), MD, but was temporarily detailed to the Adelphi Laboratory Center (ALC) in Adelphi, MD, which housed the NetBLTS unclassified servers. ALC is a DOD installation and requires government-issued identification to gain entry. Within ALC, the NetBLTS servers resided in a secure room protected by a combination lock. The servers also required a username and password in order to gain access.

* PowerEdge is a registered trademark of Dell, Inc.

† Windows is a registered trademark of Microsoft Corporation.

‡ HighView is a registered trademark of CACI International Inc.

§ Oracle is a registered trademark of Oracle Corporation.

** Microsoft Internet Information Server is a registered trademark of Microsoft Corporation.

†† Google is a registered trademark of Google Inc.

The Ground Intelligence Support Agency Command (GISA) at Ft. Bragg, North Carolina, housed the classified NetBLTS servers. Gaining entrance to GISA's secure area required users to have a higher security clearance than ALC or APG, unless they had an approved escort.

In addition to working on the nonclassified internet protocol router network (NIPRNet), the NetBLTS developers used the secret internet protocol router network (SIPRNet) to interact with the GISA personnel supporting the project. The developers accessed the SIPRNet from classified enclaves located at APG and ALC. Access to the enclaves required a security clearance. The APG and ALC enclaves are accredited for classified computing and are protected accordingly, as required by the Defense Information System Agency (DISA).

5. Information Assurance Vulnerability Alerts and Waivers

New vulnerabilities are constantly discovered in commercial off-the-shelf software. These vulnerabilities are a threat to DOD information systems. To combat and correct these threats, the DOD releases information assurance vulnerability alerts (IAVAs). An IAVA provides a compliance deadline for system administrators (SAs) to correct the vulnerability. If the compliance deadline is not met, the information system may have its Internet access revoked. All SA duties were performed by the NetBLTS team. Since the team was headquartered at APG, meeting the short compliance period was difficult because the servers were located at different locations. Getting blocked from the Internet was unacceptable for NetBLTS because of the customer requirement to maintain uptime twenty-four hours a day, seven days a week (24/7). Since NetBLTS had to maintain a 24/7 uptime, and development software would sometimes break using updated software, the NetBLTS team had to contact the information assurance manager in writing to request a special waiver that allowed NetBLTS servers to be updated manually. See appendix A for the NetBLTS waiver.

Once the waiver was in place, each time an IAVA was issued, the NetBLTS team had to submit a request to the HF management to get approval to apply the patch. This usually took time and hindered development. In addition, the team had to go through the process of backing up all of the data on the servers and determining if the patch for the vulnerability would break functionality of the translation services. Next, based on the findings and consultation with HF management, the team would seek approval to take down the servers and apply the patches.

The most difficult patches to apply were the Oracle-database patches. Because the NetBLTS team did not have direct access to the patches, it had to request the patch from a contractor. The NetBLTS team found that because of the customized Oracle installations, Oracle patches had a tendency not to execute properly and required several modifications to get them to work correctly.

Once the patches were successfully applied, the team would then bring the servers back online and thoroughly test the translation service to verify correct functionality. Only after successfully completing tests for system stability and language translation could the team let the HF community know that NetBLTS was back online and operational.

6. Gold Disks

The Gold Disks are a collection of patches stored on a compact disk that are distributed on a monthly basis by the DISA. Gold Disks provide a graphical interface that enables the user to choose one of two standards: gold or platinum. The gold standard is the minimum level of security required for network access. The platinum standard is a more restrictive level of security used for certification and accreditation. In HF, NetBLTS was required to maintain the gold standard. Periodically, a HF security representative visited the development site to verify that the gold standard was being met. The gold standard metrics per initiative/program were as follows:

- no category I findings
- no more than 20 category II findings
- arbitrary number of allowable category III findings at Designated Approval Authority discretion

An example of a category I finding is detecting a server that does not have active DOD antivirus software. A category I finding is considered critical and, if left uncorrected, would result in removing the offending service from the HF offering. There are no exceptions; correcting all category I security flaws is mandatory for reinstatement.

An example of a category II finding is detecting a server that is not enforcing the proper minimum password age. The more frequently a password is changed, the less likely it will be compromised. A category II finding is considered important and should be corrected immediately. Up to 20 category II findings are allowed, but not recommended, for continued service operation.

An example of a category III finding is detecting a server allowing remote floppy disk access. A floppy disk should be accessible solely to users who are logged onto a system locally. A category III finding is considered moderate but should still be fixed, if possible.

The NetBLTS system administrator applied appropriate patches to correct security violations. However, any Gold Disk prescribed patch had the potential to harm the functionality of system. The system administrator had to test the system after each patch to ensure correct operational capability. The Gold Disks were a key part of NetBLTS that ensured all systems were secure.

7. Auditing

HF management required that all initiatives, including NetBLTS, perform auditing to maintain usage logs. Some of the required audits and logs were automatically maintained by the operating system and were accessible using the in-place administrative tools, such as the Log Viewer.* Audits not automatically handled by the operating system required the team to develop and integrate new logging functions into the NetBLTS service. The development effort was time consuming—it required the NetBLTS team to create necessary auditing code and review the created log files to verify that all necessary functions were present and ensure that no security violations had been introduced via the solution.

The required audits/logs were as follows:

- system startup/shutdown
- authentication logon/logoff
- process invocation (when a process is started or ended)
- make an object available (bringing data online to the portfolio)
- map an object to a subject (reading data)
- object modification (modifying data)
- make an object unavailable (closing files and file systems)
- object creation (creation of data or data structures)
- object deletion (deletion of data or data structures)
- Discretionary-access-control changes
- unsuccessful data access attempt (access denials)
- actions by trusted users (admin/operator action – all service-oriented architecture [SOA] and system actions)
- insufficient privilege
- resource denials
- Interprocess communications (IPC) functions (IPC within the SOA)
- process modification

* Log Viewer is a registered trademark of Microsoft Corporation.

- audit subsystem events (changes to the HF DAC+ audit settings)
- subsystem events
- use of privilege
- authorization/permission granting (use of authorizations)
- set sensitivity label (override or modifications of data labels or markings)

For review, the NetBLTS team provided specific examples to the HF security team on how it met these requirements. The HF security team analyzed the document and, when necessary, traveled to the development site to verify compliance with the necessary auditing/logging requirements. See appendix B for the NetBLTS auditing report.

8. Conclusion

The HF program provided real-time military operational support to soldiers in the field. Therefore, the program had to adopt a zero-tolerance security policy. That decision resulted in strict security requirements for the NetBLTS initiative. Because of the combined effects of the short compliance time, the location of the servers, and not being able to access the systems remotely, security was a hindrance on the team and took away valuable time from software development. The NetBLTS team would have been better served if it initially moved the servers to APG. In the future, system security should reside with an SA whose sole job is to maintain the systems and who is co-located with the systems. By doing this, a better balance of security vs. functionality can be achieved.

Appendix A. Waiver

This appendix appears in its original form, without editorial change.

AMSRD-ARL-CI 6 October 2005

Memorandum FOR AMSRL-ALC-CI-OP, ARL Information Assurance Manager

ATTN: Dr. Stan Niles

Subject: Request for Waiver – Horizontal Fusion Program (NetBLTS)

1. Request that you approve a waiver to the ARL NetBLTS initiative, which supports the OSD Horizontal Fusion (HF) Program, from the requirement to utilize UAM, USD, and SUS software.

2. JUSTIFICATION: ARL is currently researching, developing and testing technologies necessary to enable a web-centric foreign language translation service. This service is currently instantiated in the NETBLTSDB2 and NETBLTSDB4 servers. Further, this initiative is sponsored by and under the jurisdiction of the Horizontal Fusion Project, an Office of the Secretary of Defense (OSD) and a Department of Defense (DOD) wide enterprise initiative. As such, all initiatives are directed and controlled by the Horizontal Fusion Project which has instituted a strict configuration management and control mandate on all participants. All software changes, including IAVAs, must be approved and documented by the Horizontal Fusion Configuration Control Board (CCB) in advance of application and managed and tracked via a Problem Report (PR) process. Utilization of automated means to "push" software applications or fixes is not authorized as they have the potential to disrupt the operations and the performance of any and all participants in this enterprise-wide initiative.

3. Systems under Horizontal Fusion Configuration Control are:

DB2 Related IPs:

158.12.42.45

158.12.42.46

158.12.42.100

DB4 Related IPs

158.12.42.9

158.12.42.10

158.12.42.11

158.12.42.12

158.12.42.13

The ARL NetBLTS personnel serving as System Administrators are very familiar with the policies and procedures in both the Horizontal Fusion and ARL organizations and have maintained these servers in compliance with Horizontal Fusion and ARL direction and requirements. Further, the NetBLTS IASO has consistently kept the IAM informed of NetBLTS security and IM related issues.

4. Your prompt consideration and approval of this request for waiver will be appreciated. My Action Officer is Janet F. O'May, NetBLTS IASO who can be contacted at 410 278-4998.

Eric G. Heilman
NetBLTS Project Manager
Computational & Information Science Directorate

INTENTIONALLY LEFT BLANK.

Appendix B. Auditing

This appendix appears in its original form, without editorial change.

1. **System Startup/Shutdown**
    a. **DAC+– Yes**
    b. **No DAC+ - Yes**
    c. **Hybrid - Yes**

    Notes: Standard Audit

```
2/14/2006   6:58:34 PM  USER32      Information None  1074
      NETBLTSDB4\testuser     NETBLTSDB4  "The process Explorer.EXE has
initiated the restart of computer NETBLTSDB4 on behalf of user
NETBLTSDB4\testuser for the following reason: Other (Planned)
Reason Code: 0x85000000
Shutdown Type: restart
Comment: Patches"
```

2. **Authentication Logon/Logoff**
    a. **DAC+– Yes**
    b. **No DAC+ - Yes**
    c. **Hybrid - Yes**

    Notes: Standard Audit

    Sample SOA Event:

    Logging on to a system
    Logging off a system
    Validating a Server/Client Certificate
    Validating a SAML assertion
    Message signature verification (success/fault)
    Certification validation and status checking results (success/fault)

```
3/14/2006      6:44:48 PM  Security    Success Audit     Logon/Logoff
   538   NETBLTSDB4\testuser     NETBLTSDB4  "User Logoff:
   User Name:  testuser
   Domain:           NETBLTSDB4
   Logon ID:         (0x0,0x9B7149E)
   Logon Type: 7

Or

13 Mar 2006 20:46:16,171 DEBUG [CertValidationHelper] validateChain():
subjectDN = "CN=hfdevportal4.spawar.navy.mil, OU=USN, OU=PKI, OU=DoD,
O=U.S. Government, C=US" issuerDN = "CN=DOD CLASS 3 CA-7, OU=PKI, OU=DoD,
O=U.S. Government, C=US" serial = 135896

13 Mar 2006 20:46:16,171 DEBUG [CertValidationHelper] validateChain():
Direct trust for certificate with "CN=hfdevportal4.spawar.navy.mil,
OU=USN, OU=PKI, OU=DoD, O=U.S. Government, C=US"
13 Mar 2006 20:46:16,171 DEBUG [CertValidationHelper] Looking for CN=DOD
CLASS 3 CA-7, OU=PKI, OU=DoD, O=U.S. Government, C=US.135896 in [CN=DoD
CLASS 3 Root CA, OU=PKI, OU=DoD, O=U.S. Government, C=US.4, CN=DOD CLASS 3
JITC CA-7, OU=PKI, OU=DOD, O=U.S. Government, C=US.2420, CN=JITC DoD PKI
Class 3 Root CA, OU=PKI, OU=DoD, O=U.S. Government, C=US.69, CN=JITC DoD
PKI Class 3 Root CA, OU=PKI, OU=DoD, O=U.S. Government, C=US.4,
CN=ca.boozallenET.com.738006208007647759756491674563792623336, CN=DOD CLASS
```

```
3 CA-7, OU=PKI, OU=DoD, O=U.S. Government, C=US.135896, CN=BAH LAB TEST
ROOT ECA, OU=PKI, OU=DoD, O=U.S. Government, C=US.20, CN=BAH LAB TEST ROOT
ECA, OU=PKI, OU=DoD, O=U.S. Government, C=US.5, CN=DoD CLASS 3 Root CA,
OU=PKI, OU=DoD, O=U.S. Government, C=US.33, CN=DOD CLASS 3 CA-7, OU=PKI,
OU=DoD, O=U.S. Government, C=US.132349]..answer = true
13 Mar 2006 20:46:16,171 DEBUG [NCESServerHandler] Cert is trusted.. We
can skip the certificate validation step.
13 Mar 2006 20:46:16,171 DEBUG [NCESServerHandler] Just put this security
info in the context
Asserter = Web Service Handler
Subject = CN=RICHARDSON.JOHN.T.1270046440,OU=USA,ou=pki, ou=dod, o=U.S.
Government, c=us
Subject Clearance = [S]
Subject Citizenship = [USA]
Message Classification = [S]
Message NonUSClassification = []
Message DisseminationControl = [NOFORN]
Message releasableTo = []
Security Roles = [user.analyst, user.operator]
Time to Live = 600000
Sign Preference = true
```

3. **Process Invocation (when a Process is started or ended)**
    a. **DAC+– Yes**
    b. **No DAC+ - Yes**
    c. **Hybrid – N/A**

Notes: Should be limited to security handlers

Sample SOA Event:

Application initialization from the Portal
Session Initialization
Security Handler Start Up

```
14 Mar 2006 12:00:56,640 DEBUG [NCESServerHandler] Are we checking for
messageID?true
14 Mar 2006 12:00:57,250 DEBUG [NCESMessageValidator] constructor: loading
crypto
14 Mar 2006 12:00:57,250 DEBUG [SecurityLoader] SecurityLoader Starting..
14 Mar 2006 12:00:57,265 DEBUG [SecurityLoader] Loaded property file:
file:/D:/Tomcat5/webapps/axis/WEB-INF/classes/diaSecurity.properties
```

4. **Make an Object Available (Bringing data online to the Portfolio)**
    a. **DAC+– Yes**
    b. **No DAC+ - No**
    c. **Hybrid – As Required**

Notes: Each time a process opens a file or mounts a file system. Audit should be limited to Volume events to control the number of events.

Sample SOA Event:

Volume mounts
Opening data containers

```
<netbltsServices service_name="NetBLTS2" action="retrieval" status="success"
```

```
host_servername="netbltsdb4.arl.army.mil" user="netblts" object_id="26830"
time="05471602022006">DocexFS WebServices Retrieve Document</netbltsServices>
```

5. **Map an Object to a Subject (reading data)**
    a. **DAC+– Yes**
    b. **No DAC+ - No**
    c. **Hybrid – As Required**

    Notes: Each time a process reads a file or data, URL. This would be too voluminous.

```
7 Mar 2006 19:27:58,234 DEBUG [ProxyProperties] passwordfilelocation:
"D:\\Tomcat5\\webapps\\axis-out\\WEB-INF\\PasswordsEncrypted.txt"
07 Mar 2006 19:27:58,250 DEBUG [ProxyProperties]
 now, check standard ssl system properties, again, after new code was
executed...
07 Mar 2006 19:27:58,250 DEBUG [ProxyProperties] javax.net.ssl.keyStore :
D:\\Certs\\service-consumer.jks
07 Mar 2006 19:27:58,250 DEBUG [ProxyProperties] javax.net.ssl.trustStore :
D:\\Certs\\caTrustStore.jks
07 Mar 2006 19:27:58,250 INFO  [ProxyProperties] Initializing Proxy As Client
[End]
07 Mar 2006 19:27:58,250 DEBUG [secureProxy] Done with setting values...
```

6. **Object Modification (modifying data)**
    a. **DAC+– Yes**
    b. **No DAC+ - No**
    c. **Hybrid – As Required**

    Notes: Each time a process modifies the data in a file or changes the file's or data's attributes.

    Sample SOA Event:

    Limited to label changes

```
N/A
```

7. **Make an Object Unavailable (closing files and file systems)**
    a. **DAC+– Yes**
    b. **No DAC+ - No**
    c. **Hybrid – As Required**

    Notes: Each time a process closes a file, dismounts a file system, etc. Audit should be limited to volume events to control the number of events.

    Sample SOA Event:

    Dismounts

    Closing data containers

```
Shutting down instance: further logons disabled
Shutting down instance (immediate)
License high water mark = 3
Waiting for dispatcher 'D000' to shutdown
All dispatchers and shared servers shutdown
Thu Feb 03 16:36:16 2005
ALTER DATABASE CLOSE NORMAL
Thu Feb 03 16:36:17 2005
```

```
SMON: disabling tx recovery
SMON: disabling cache recovery
Thu Feb 03 16:36:17 2005
Shutting down archive processes
Archiving is disabled
Archive process shutdown avoided: 0 active
Thread 1 closed at log sequence 1
Successful close of redo thread 1
Thu Feb 03 16:36:17 2005
Completed: ALTER DATABASE CLOSE NORMAL
Thu Feb 03 16:36:17 2005
ALTER DATABASE DISMOUNT
Completed: ALTER DATABASE DISMOUNT
ARCH: Archiving is disabled
Shutting down archive processes
Archiving is disabled
Archive process shutdown avoided: 0 active
ARCH: Archiving is disabled
Shutting down archive processes
Archiving is disabled
Archive process shutdown avoided: 0 active
```

8. **Object Creation (creation of data or data structures)**
    a. **DAC+– Yes**
    b. **No DAC+ - Yes**
    c. **Hybrid - Yes**

Notes: Whenever a file, directory, or link are created (and thus labeled).

Sample SOA Event:

Query response (found set)

```
<netbltsServices service_name="NetBLTS2" action="creation" status="success"
host_servername="netbltsdb4.arl.army.mil" user="netblts" object_id="27765"
time="01415502012006">Docex WebServices Create Document</netbltsServices>
```

9. **Object Deletion (deletion of data or data structures)**
    a. **DAC+– Yes**
    b. **No DAC+ - No**
    c. **Hybrid – As Required**

Notes: Whenever a file, directory, or link are deleted.

```
Production NetBLTS Server deletes test data entered into the Oracle database
manually.
```

10. **DAC Changes**
    a. **DAC+– Yes**
    b. **No DAC+ - Yes**
    c. **Hybrid - Yes**

Notes: Changes to the DAC+ settings that determine what events are being captured.

```
This is a manual process for NetBLTS. A log book is kept on site.
```

```
Ex. (Username) (date) (time) (old dac+ mode) (new dac+ mode) (comments)
```

11. Unsuccessful Data Access Attempt (Access Denials)

- **a. DAC+– Yes**
- **b. No DAC+ - No**
- **c. Hybrid – As Required**

Notes: Whenever an access failure occurs.

```
14 Mar 2006 14:35:33,593 DEBUG [NCESSecurityException]
NCESSecurityException(): message = "The user did not have the authorized role
to access this web service." cause = null
```

12. Actions by Trusted Users (Admin/Operator Action – All SOA and System Actions)

- **a. DAC+– Yes**
- **b. No DAC+ - Yes**
- **c. Hybrid - Yes**

Notes: Major actions by the administrator.

Sample SOA Event:

User definition
Role creations
Changes or deletions

```
11/29/2005  5:49:47 PM  Security    Success Audit     Account Management
      624   NETBLTSDB4\testuser     NETBLTSDB4  "User Account Created:
      New Account Name: moss
      New Domain: NETBLTSDB4
      New Account ID:   %{S-1-5-21-385639716-758612822-3886322124-1053}
      Caller User Name: testuser
      Caller Domain:    NETBLTSDB4
      Caller Logon ID:  (0x0,0x2BE16)
      Privileges        -
 Attributes:
      Sam Account Name: moss
      Display Name:     <value not set>
      User Principal Name:    -
      Home Directory:   <value not set>
      Home Drive: <value not set>
      Script Path:      <value not set>
      Profile Path:     <value not set>
      User Workstations:      <value not set>
      Password Last Set:      <never>
      Account Expires:  <never>
      Primary Group ID: 513
      AllowedToDelegateTo:    -
      Old UAC Value:    0xAF4D0
      New UAC Value:    0xAF4D0
      User Account Control:   -
      User Parameters:  <value not set>
      Sid History:      -
      Logon Hours:      <value changed, but not displayed>
```

13. Insufficient Privilege

a. **DAC+– Yes**
b. **No DAC+ - Yes**
c. **Hybrid - Yes**

Notes: A program calls for an object that the requesting user does not have the privilege for.

Sample SOA Event:

Non US role attempting to access US data

```
13 Mar 2006 16:38:44,250 DEBUG [CertValidationHelper] Getting
SecurityTokenReference... Looking for {http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd}SecurityTokenReference
13 Mar 2006 16:38:44,250 DEBUG [CertValidationHelper] validateChain():
subjectDN = "CN=hfdevportal4.spawar.navy.mil, OU=USN, OU=PKI, OU=DoD, O=U.S.
Government, C=US" issuerDN = "CN=DOD CLASS 3 CA-7, OU=PKI, OU=DoD, O=U.S.
Government, C=US" serial = 135896

13 Mar 2006 16:38:44,250 DEBUG [CertValidationHelper] validateChain():
Couldn't find certificate with serial number 135896 from issuer "CN=DOD CLASS
3 CA-7, OU=PKI, OU=DoD, O=U.S. Government, C=US"
```

14. Resource Denials

a. **DAC+– N/A**
b. **No DAC+ - N/A**
c. **Hybrid – N/A**

Notes: This is not necessary in HF because these classes of events tend to be system tuning.

```
N/A
```

15. IPC Functions (interprocess communication within the SOA)

a. **DAC+– Yes**
b. **No DAC+ - Yes**
c. **Hybrid – As Required**

Notes: These are successes and failures of communications among SOA participants.

Sample SOA Event:

Outbound message information (message ID, sending timestamp, Host, target service)

Inbound messaging information (message ID, receiving timestamp)

```
07 Mar 2006 19:27:58,281 DEBUG [BindingCacheAdapter] BindingCacheAdapter()
serviceProfileName: CertificateValidationService
07 Mar 2006 19:27:58,281 DEBUG [BindingCacheAdapter]
[BindingCacheAdapter.initialize] Initializing UDDI Binding Cache at:
http://localhost:8945/BindingCache/BindingCache.asmx
07 Mar 2006 19:27:58,312 DEBUG [BindingCacheAdapter] Got Binding Cache Soap
stub.
07 Mar 2006 19:28:02,875 DEBUG [BindingCacheAdapter] Received 2 endpoints
from UDDI binding cache.
07 Mar 2006 19:28:02,890 DEBUG [BindingCacheAdapter]
```

```
BindingCacheAdapter:isValidEndpt: connected to endpoint:
https://hfsws2.spawar.navy.mil/securityPIE/services/CertificateValidationServ
ice
```

16. **Process Modification**
    a. **DAC+– N/A**
    b. **No DAC+ - N/A**
    c. **Hybrid – N/A**

Notes: This isn't used in HF because all processes run at the highest level of the system. However, we could consider auditing whenever an application is changed or restarted.

```
N/A
```

17. **Audit Subsystem Events (changes to the HF DAC+ audit settings)**
    a. **DAC+– Yes**
    b. **No DAC+ - Yes**
    c. **Hybrid - Yes**

Notes: Changes to Audit Events Configuration. This assumes HF making the audit events configurable.

Sample SOA Event:

OS Audit Diagraph Changes

```
20 Mar 2006 19:54:48,656 INFO  [CPDSServerHandler] DAC+ mode set to: hybrid
```

18. **Subsystem Events**
    a. **DAC+– N/A**
    b. **No DAC+ - N/A**
    c. **Hybrid – N/A**

Notes: This isn't used in HF because all processes run at the highest level of the system.

```
N/A
```

19. **Use of Privilege**
    a. **DAC+– Yes**
    b. **No DAC+ - Yes**
    c. **Hybrid - Yes**

Notes: The use or attempted use of privilege. The use of privilege would be voluminous.

Sample SOA Event:

Policy decision results (permit/deny/indeterminate)

```
07 Mar 2006 19:28:02,937 DEBUG [ProxyClientAppender] About to create a
security object for -CN=DOD CLASS 3 JITC CA-7, OU=PKI, OU=DOD, O=U.S.
Government, C=US-
07 Mar 2006 19:28:02,937 DEBUG [ProxyClientAppender] Add role
07 Mar 2006 19:28:02,937 DEBUG [ProxyClientAppender] Add clearance
07 Mar 2006 19:28:02,937 DEBUG [ProxyClientAppender] Add citizenship
```

```
07 Mar 2006 19:28:02,937 DEBUG [ProxyClientAppender] Add classification
07 Mar 2006 19:28:02,937 DEBUG [ProxyClientAppender] Add dissemination
07 Mar 2006 19:28:02,937 DEBUG [ProxyClientAppender] Add NonUSClass
07 Mar 2006 19:28:02,937 DEBUG [ProxyClientAppender] Add ReleasableTo
07 Mar 2006 19:28:02,953 DEBUG [NCESMessageBuilder] constructor, setting
sinfo to Asserter =
Subject = CN=DOD CLASS 3 JITC CA-7, OU=PKI, OU=DOD, O=U.S. Government, C=US
Subject Clearance = [S]
Subject Citizenship = [USA]
Message Classification = [U]
Message NonUSClassification = []
Message DisseminationControl = []
Message ReleasableTo = []
Security Roles = [user.operator]
Time to Live = 600000
Sign Preference = true
```

20. Authorization/Permission granting (Use of Authorizations)

- **a. DAC+– Yes**
- **b. No DAC+ - Yes**
- **c. Hybrid - Yes**

Notes: The use or attempted use of Authorization. The use of authorization would be voluminous. This should be limited to Failures.

```
14 Mar 2006 14:37:53,343 DEBUG [NCESServerHandler] beging to check for
filtered IP.
14 Mar 2006 14:37:53,343 DEBUG [NCESServerHandler] Either we are disallowing
trusted IP access or the IP address is not in the list.
```

21. Set Sensitivity Label (override or modifications of data labels or markings)

- **a. DAC+– Yes**
- **b. No DAC+ - No**
- **c. Hybrid – As Required**

Notes: Establishments or Change to any label.

Sample SOA Event:

Consolidating a found set and labeling
Change metadata label
Initial labeling

13 Mar 2006 16:24:35,171 INFO [CPDSServerHandler] getMessageSecurityType()
13 Mar 2006 16:24:35,171 DEBUG [CPDSServerHandler] getMessageSecurityType: Message classification: U
13 Mar 2006 16:24:35,171 DEBUG [SecurityTypeUtils] U found in validity cache, value = true
13 Mar 2006 16:24:35,171 DEBUG [SecurityTypeUtils] S NOFORN found in validity cache, value = true
13 Mar 2006 16:24:35,171 INFO [CPDSServerHandler] clearance of S NOFORN dominates U
13 Mar 2006 16:24:35,171 INFO [CPDSServerHandler] Service accredited.max TS NOFORN dominates U

NO. OF
COPIES ORGANIZATION

1 (PDF ONLY) DEFENSE TECHNICAL INFORMATION CTR
DTIC OCA
8725 JOHN J KINGMAN RD
STE 0944
FORT BELVOIR VA 22060-6218

1 US ARMY RSRCH DEV & ENGRG CMD
SYSTEMS OF SYSTEMS INTEGRATION
AMSRD SS T
6000 6TH ST STE 100
FORT BELVOIR VA 22060-5608

1 DIRECTOR
US ARMY RESEARCH LAB
IMNE ALC IMS
2800 POWDER MILL RD
ADELPHI MD 20783-1197

3 DIRECTOR
US ARMY RESEARCH LAB
AMSRD ARL CI OK TL
2800 POWDER MILL RD
ADELPHI MD 20783-1197

ABERDEEN PROVING GROUND

1 DIR USARL
AMSRD ARL CI OK TP (BLDG 4600)

NO. OF
COPIES ORGANIZATION

ABERDEEN PROVING GROUND

25 DIR USARL
AMSRD ARL CI
J GOWENS
AMSRD ARL CI C
A CLARK
AMSRD ARL CI CB
L TOKARCIK
AMSRD ARL CI CT
T HANRATTY
E HEILMAN
R KASTE
M MITTRICK (15 CPS)
G MOSS
J O'MAY
J RICHARDSON
M THOMAS

INTENTIONALLY LEFT BLANK.